

STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)
Section:	06	Title: Information Security
Sub Section:	05	Title: Communications
Document:	05	Title: Voice

1. STANDARD

ISD will institute security measures to avoid the possibility of theft or misuse of either phone service or information through the telephone systems.

1.1. Summary of Standard Changes

1.2. Purpose

Protect the ISD PBX and its processes from fraudulent or unauthorized use.

1.3. Scope

Applies to all PBX processes and the employees and public which use them.

1.4. Responsibilities

1.5. Definitions and Abbreviations

1.6. Description of Standard

The dial-up modem maintenance port will be protected from unauthorized access. Direct inward system access (DISA) will not be allowed through the ISD private branch exchange (PBX). Unauthorized long distance calling will not be allowed. Protection of, and fraudulent use of voice mail will be minimized through proper procedures.

1.7. Implications

ISD will control and monitor use of the PBX to minimize fraudulent and unauthorized use of systems, or misuse of information.

1.8. References

1.9. Attachments

2. DIAL-UP MAINTENANCE PORT PROCEDURES

2.1. Summary of Procedure Changes

2.2. Procedure Details

The following steps are taken to protect the dial-up modem maintenance port from unauthorized access:

- 2.2.1. The default or manufacturer's password coming with the system will be changed to one known only by maintenance personnel.

STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)
Section:	06	Title: Information Security
Sub Section:	05	Title: Communications
Document:	05	Title: Voice

2.2.2. Passwords will conform to ISD standards (re: Section 6, Sub-section 3, Document C - Passwords) where possible.

2.2.3. Maintenance port is shut off when not in use.

2.2.4. Maintenance port activity reports are created and inspected for abnormal usage.

2.2.5. System maintenance records and correspondence will be monitored for abnormal activity.

2.3. References

2.4. Attachments

3. DIRECT INWARD SYSTEM ACCESS (DISA) PROCEDURES

3.1. Summary of Procedure Changes

3.2. Procedure Details

Access to the ISD PBX through 800 numbers or local dial-in to gain access to long distance lines is blocked to all.

3.3. References

3.4. Attachments

4. CLASS OF SERVICE SCREENING PROCEDURES

4.1. Summary of Procedure Changes

4.2. Procedure Details

4.2.1. Unauthorized long distance calling will be restricted at the PBX in the following circumstances:

4.2.1.1. All international calling for employees without authority.

4.2.1.2. All 900 and 976 numbers having charges.

4.2.1.3. All 950 carrier codes when possible for card access to other carriers.

STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)
Section:	06	Title: Information Security
Sub Section:	05	Title: Communications
Document:	05	Title: Voice

4.2.1.4. All 10XXX carrier calls for carriers other than the one of choice.

4.2.2. Long distance call records will be monitored for unauthorized call usage.

4.2.3. Line usage will be monitored to discover possible open modem line misuse.

4.3. References

4.4. Attachments

5. VOICE MAIL PROCEDURES

5.1. Summary of Procedure Changes

5.2. Procedure Details

The following steps will be used to minimize fraudulent voice mail use:

5.2.1. Only allow external incoming calls to be transferred to outside lines through programmed controls.

5.2.2. Passwords will conform to ISD standards (re: Section 6, Sub-section 3, Document C - Passwords) where possible.

5.2.3. Unassigned mailboxes will be deleted.

5.2.4. Voice mail will be monitored for authorized security purposes.

5.3. References

5.4. Attachments